UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ADAM PEZEN, individually and on behalf of all others similarly situated, *Plaintiff*, v. FACEBOOK, INC., *Defendant*.	Case No.

CLASS ACTION COMPLAINT

Plaintiff Adam Pezen ("Plaintiff"), individually and on behalf of all others similarly situated (as defined below), by Plaintiff's undersigned attorneys, brings this Class Action Complaint against Defendant, Facebook, Inc. ("Facebook"), alleging based on personal knowledge as to himself, and upon information and belief as to all other matters based on the investigation of counsel.

NATURE OF THE ACTION

1. This case arises out of the misuse by Defendant Facebook, the largest social media network in the world, of personally identifying biometric information that Facebook collected from its members, without their informed consent, in clear violation of Illinois law.

2. More specifically, Facebook has collected and stored millions of face templates from its users. Face templates are digital maps of facial points which are sometimes referred to in the biometric industry as "face prints," which is a digital biometric template specific to facial recognition technology. Facebook extracts geometric data from photos uploaded by Facebook members to create a highly detailed geometric map (i.e., the "face template") of the user's face.

Every face template is unique to the individual to whom it belongs, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person (within a reasonable margin of error). Together, this kind of strong identity information is known as "biometric" information.

3. Facebook has collected and used this data on a massive scale under its facial biometric system, which is integrated into Facebook's Photo Tag Suggest (hereafter "PTS") program, without informed consent from its members, and with no meaningful effort made to provide clear information to its members about what Facebook is doing and how its members are affected.

4. The large-scale collection of this type of sensitive information without informed consent raises serious privacy concerns and violates the Biometric Information Privacy Act ("BIPA"). Face templates such as those that Facebook has gathered are known as "strong identifiers," and constitute highly sensitive and personal data with a large potential for misuse. Face templates can be used, for example, to scan millions of digital photographs or images from security cameras to locate an individual via face template comparison and matching, or conversely, can be used to gain access to all detailed information about an otherwise anonymous individual using face template comparisons. Moreover, unlike other identifying information, such as a social security or credit card number, a face template, like a fingerprint, is a biological identifier, which means it is unique to each specific individual and cannot be easily changed.

5. Because of the high potential for abuse and because of the potential for security risks to individuals, the Illinois legislature saw fit to protect residents of Illinois by respectively enacting and signing into law the BIPA in 2008. The BIPA prohibits any private entity from collecting, capturing or otherwise obtaining a person's biometric information, which specifically includes "face geometry," without first obtaining informed written consent from the individual.

Facebook has clearly violated (and continues to violate) the statute because it collects the precise type of biometric data contemplated by the BIPA from its members without first obtaining the required informed, written consent from individuals whose data it collects. The BIPA also requires that any private entity, such as Facebook, in possession of biometric data "must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information …" Facebook has not made any such written policy (if it has one) available to the public as required. Therefore, in these ways and as otherwise described in greater detail below, Defendant Facebook has violated the BIPA and the privacy rights of members of the Illinois public.

PARTIES

6. Defendant Facebook is a Delaware corporation headquartered at 1601 Willow Road, Menlo Park, California 94025. Facebook is also registered to conduct business in the State of Illinois (file number 66267067), and maintains an office in Cook County in the State of Illinois.

7. Plaintiff Adam Pezen is a natural person residing in Cook County in the State of Illinois.

JURISDICTION AND VENUE

8. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA"), because (i) the proposed Class consists of well over 100 members; (ii) the parties are minimally diverse, as members of the proposed Class, including Plaintiff, are

citizens of a state different from Defendant's home states; and (iii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs.[1]

9. This Court has personal jurisdiction over Plaintiff because Plaintiff submits to the Court's jurisdiction. This Court has personal jurisdiction over Defendant Facebook because Defendant is registered to conduct, and does in fact conduct, substantial business throughout Illinois, including in this District, and Defendant maintains and uses an office in this District. Defendant thus has sufficient minimum contacts with this District and Illinois. In addition, Plaintiffs' claims arise out of Defendant conducting and transacting business in Illinois, and many of the actions giving rise to the Complaint took place in this District.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant Facebook is a resident of this District and is subject to this Court's personal jurisdiction. Defendant Facebook is registered to conduct business throughout Illinois, regularly conducts business in this District, and maintains an office in this District. In addition, the causes of action arose, in substantial part, in this District, and Plaintiff resides in this District.

FACTUAL BACKGROUND

I. Facebook's Business Model

11. Facebook is the largest online social network in the world, with over half a billion active users, and approximately seven million users in Illinois alone. Facebook's members establish a user profile by posting personal information about themselves that may include the member's e-mail address, phone number, birthday, religious and political beliefs, gender and

[1] As of August 2010, there were over seven million Facebook users in Illinois. *See* Internet World Stats, *United States of America Internet and Facebook User Stats*, http://www.internetworldstats.com/stats26.htm (last visited April 20, 2014). This number has likely only increased in the last five years. Nevertheless, even a conservative estimate of the number of Illinois Facebook users impacted by Defendant's conduct, as alleged herein, multiplied by BIPA's statutory liquidated damages figure, easily exceeds CAFA's $5,000,000 threshold, and therefore represents a good-faith, plausible estimate of the amount in controversy that is, undoubtedly, legally possible.

sexual orientation, and other kinds of personal information. After their user profile is established, users can interact with other members on Facebook's network by communicating with each other through messages or comments, or by uploading photographs of themselves that may become visible to others.

12. An essential element of the Facebook network that encourages its members to post all of this personal and sensitive information is that members are supposed to be able to maintain control over that information. Facebook's Privacy Settings are where members are supposed to be able to maintain control over that information by deciding whether to make it fully public, or accessible only to other members or a subset of members.

13. User-uploaded photographs have become a key component of Facebook's business. As of October 2012, Facebook maintained approximately 220 billion user-uploaded photographs on its network, and that number increases by up to approximately 300 million photographs every day. Facebook, like other social network sites, has found that users are more likely to engage with posts and comments that are associated with photos. This is important, because Facebook's business model depends on its ability to maintain and increase user engagement, as it must compete for customer loyalty with other social networking sites.

14. Facebook is the undisputed juggernaut of social media and is the largest photo sharing site in the world by a wide margin. Facebook's dominance ensures that it continues to receive a steady stream of revenue from advertising and other partnerships. In 2014 alone, Facebook generated more than $12 billion in revenue.

II. How Facebook's Photo Tag Suggest Feature Works

15. One of the ways in which Facebook increases user engagement is by allowing members to "tag" themselves or others in photographs they upload. Tags identify who is in the photo, and where in the photo those individuals are located. Tags also typically act as

hyperlinks, which, if clicked on, will take the user directly to the profile of the member that is tagged in the photo. Conversely, a user can start at a profile page of a particular member and, subject to various privacy settings, view all the photos in which that member is tagged in one place, regardless of who uploaded or tagged the photo. Tags can, therefore, increase user engagement by increasing the number of people that can easily locate and gain access to photos of members that are stored in various locations on Facebook's network.

16. Basic photo tagging has been available on Facebook since the relatively early days of the company's existence. In 2011, however, Facebook began to roll out the PTS feature. PTS utilizes state of the art facial recognition technology to create a digital face template that maps the unique geometry of a member's face and stores it in a database together with millions of other digital face templates.

17. PTS is a complex system that operates at a number of layers. An important aspect of PTS is that it uses a sample of training images, or "Photo Comparison Data," which consist of photos uploaded by members that have previously been manually tagged by users. Facebook uses its proprietary facial recognition software to analyze and compare the faces of the tagged individuals in those training images. As more images are uploaded and tagged, the computational accuracy of Facebook's PTS increases. By using many photos of the same individual, the PTS software compares different images of the same person's face with varying light, distance, angle, resolution, and facial expression. The PTS software, according to Facebook, "compare[s] what these tagged photos have in common and store[s] a summary of this comparison." The "summary of this comparison" Facebook is referring to here is what in the industry is known as the face template. Facebook stores the face templates in a database that is inaccessible to the

user, but which can be used by Facebook to analyze and compare other photographs to automatically detect and identify the user's face.

18. Facebook spent a great deal of resources to develop and collect the PTS database and analysis system. Facebook acquired an Israeli start-up called Face.com for an estimated $80-$100 million to obtain the sophisticated and nuanced facial recognition software used in Facebook's PTS feature.

III. Facebook Creates Digital Face Templates Without Informed Written Consent

19. Facebook began to collect its users' biometric facial data in preparation for the PTS roll-out sometime between approximately December 15, 2010 and June 7, 2011, but has never disclosed when exactly the data extraction began. Instead, Facebook simply announced that the PTS program had begun ***after*** it was already under way.

20. During this first phase of data collection Facebook gave no specific notice to users about the collection and analysis of facial templates, and failed to obtain consent prior to collecting "Photo Comparison Data," generating strong biometric identifiers, and linking biometric templates with individual users.

21. Facebook later admitted that "we should have been more clear during the roll-out process when this became available" to their users. However, despite this admission, Facebook has since that time made a de minimis effort to provide information about the PTS program to its members, and has **never obtained informed written consent from any resident of Illinois whose facial templates have been, and continue to be, captured and analyzed by Facebook**. Even to this day, Facebook does not obtain informed consent, written or otherwise, from its US-based members prior to extracting, using and storing their biometric face templates.

22. Instead, Facebook has set as a default setting that PTS is automatically enabled on users' accounts (within the United States) without any specific prior notification or informed

written consent. Unlike other Facebook features that provide the user with information up front about the feature and prompt the user's consent before activation, PTS provides no such information and requests no such consent. For example, Facebook's "Nearby Friends" feature provides four full screens of highly specific consumer education about the Nearby Friends feature, which uses geolocation to identify which of a user's friends are nearby at any given moment. The fourth and final consumer education screen has two prominent and clear selection buttons, one labeled "Not Now" and the other labeled "Turn On."[2]

23. Further, Facebook provides only a highly convoluted methodology accompanied by imprecise wording for turning the PTS feature off and deleting the biometric information that Facebook has already collected, stored and used, after the fact. Beyond the convoluted path to the opt out, the descriptions Facebook uses to describe the process of deleting the face template is "turn off tag suggestions." The phrase "turn off tag suggestions" in the immediate opt-out box area is appreciably inadequate to notify consumers that turning off this feature will result in the deletion of a biometric face template, which, as discussed, is a strong identity technology of significant sophistication and potential consequence.

24. The process for turning off tag suggestions must be actively sought out by the user, meaning that the user must first be aware of what is happening, which Facebook impedes by providing only bare information about PTS in remote parts of its website. Further, the descriptions in the immediate area around turning off tag suggestions are not specific to the fact that choosing certain options will delete stored biometric facial templates.

25. For much of the time the PTS feature existed, the notification of how to have one's biometric data deleted from Facebook was actually incorrect, and would send users on a

[2] Facebook's features, notifications and processes can vary somewhat depending on the version and method of access.

wild goose chase around Facebook's website in a futile attempt to have the information removed, that would ultimately end in no option other than sending a message to the Facebook "Photos Team" requesting the deletion and waiting for a response. Even today, having one's biometric data retroactively deleted from Facebook's database requires (i) knowing that such data is being stored by Facebook in the first place, (ii) seeking out and finding on a buried section of the website the instructions for turning off tag suggestions, (iii) following the instructions to navigate to a different part of Facebook's website, and (iv) selecting the correct option from a drop-down menu. Moreover, the Facebook menu option that creates the deletion of a users' biometric facial template does not clearly state that the menu option deletes a biometric facial template within the immediate option area where a user is making a choice about the biometric facial template.

26. Finally, even people who are not Facebook users have had their biometric data stored on Facebook; and these non-users have clearly never provided any informed consent. When a Facebook user uploads a photo of a non-user and tags the non-user, the non-user will not know that their facial template has been created on Facebook, and stored in what has been called "shadow profiles" or "shadow accounts." Even when a photo of a non-user is simply uploaded and not manually tagged, it is still going to be analyzed by Facebook's facial recognition technology. Two significant investigations of Facebook by the Irish and Belgian European Data Protection Commission offices documented that Facebook is gathering data on non-users, including data obtained from photos. Articles in major media have publicly discussed Facebook's collection of non-user data through shadow profiles, and technical publications have described the specifics of how Facebook collects and amasses non-user data.

IV. Facebook's Conduct is a Clear Violation of the Biometric Information Privacy Act on a Massive Scale

27. The Illinois BIPA is a straightforward statute designed to protect the privacy rights of Illinois citizens. Facebook, through its PTS program as described in this Class Action Complaint, has flagrantly and repeatedly violated the BIPA.

28. Section 15(b) of the BIPA provides that:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> > (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
> >
> > (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and***
> >
> > (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

29. "Biometric information" is defined as "any information regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual," and "biometric identifier" is defined to specifically include any "scan of … face geometry." 740 ILCS 14/10. "Written release" is defined in the statute as "informed written consent." *Id.*

30. Facebook utterly failed (and continues to fail) to comply with any of these BIPA requirements. *First*, Facebook did not inform its users that it was collecting their biometric information and creating face templates before it began doing so. Even after the PTS roll-out was publicly disclosed, Facebook made no attempt to actually "inform[] the subject" (*i.e.* the Facebook user) by providing specific, clear notice to users (or non-users) whose information it

was capturing. *Second*, Facebook did not inform its users of the "specific purpose" for which the biometric information was being collected, nor did it inform its users how long it would be collecting and storing this information. *Third*, Facebook has never received, much less sought out, the informed consent of any of its users, written or otherwise, prior to collecting their biometric information.

31. Facebook has failed to satisfy ***all three prongs*** of BIPA and therefore has plainly violated the statute. In fact, Facebook has violated BIPA countless times, because it does so each time it collects the biometric information of any Illinois citizen, regardless of where in the world that Illinois citizen is at the time that data is collected, and regardless of whether that Illinois citizen is a Facebook user.

32. Additionally, Section 15(a) of the BIPA provides that any

> private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

33. Facebook has no such publicly available written policy for the permanent destruction of the biometric information that it collects from users, and certainly not one that complies with Section 15(a). Defendant has therefore violated this subsection of the BIPA as well.

V. Facebook's Numerous Violations of the Biometric Information Privacy Act are Intentional or Reckless

34. Facebook did not accidentally gather biometric information from its members from their photographs, create and store face templates of each of them, and then use those face templates to locate the users in other pictures. Rather, Facebook's development and

implementation of the PTS program was very deliberate, costing Facebook tens of millions of dollars and years of labor. Facebook's conduct was, therefore, intentional.

35. Indeed, Defendant Facebook has been consciously disregarding the privacy rights of its members for years and doggedly refused to change its notice or consent policies. Perhaps the clearest evidence of this is that the PTS feature is no longer operational for Facebook users in Europe after intense criticism from several European regulators that found that PTS violated the privacy rights of users.

36. Moreover, in 2011, Facebook itself publicly acknowledged the privacy-related failures of the PTS program, conceding that there was a lack of clarity surrounding the program. Despite this, Facebook has done virtually nothing to change its policies so as to provide users with adequate information or seek their consent before harvesting their highly sensitive biometric data.

37. Facebook's implementation of the PTS software without its members' consent also displays a reckless disregard for the privacy rights of its members. Despite Facebook's attempts to portray PTS as no more than a benign tool to make user experience more enjoyable, biometric user information such as the massive facial template database that Facebook has collected is no trifling matter, and has the potential to cause harm to its members. Facebook knows this full well from, *inter alia*, its participation at many industry conferences in which these topics have been raised.

38. As the Federal Trade Commission ("FTC") acknowledged in 2012, because facial recognition technology "holds the prospect of identifying anonymous individuals in public," it is important that companies using this technology inform consumers and provide them with a choice as to whether this facial-feature data can be collected. Facebook's failure to issue detailed

information about how it collects, stores and uses biometric information is all the more troubling because of how dangerous that information could be in the wrong hands, especially a database of such information as massive as the one that Facebook has collected covering a huge percentage of our society. In addition to the risk that this information could be obtained by criminals ranging from identity thieves to kidnappers and terrorists, there is also a gross lack of transparency over how Facebook permits hundreds of thousands of business partners to use its data. Facebook permits a certain amount of its users' data to be used by third parties that may be either advertising on Facebook and hoping to target users based on their personal information, or developing applications or "apps" that users interact with within Facebook's network. Facebook does not always maintain prudent control over these third parties, however, such as when one advertiser was caught using profile pictures in singles dating service advertisements, and Facebook responded simply by stating that the ads came "from rogue networks." Additionally, although Facebook does not allow "site scraping" (the unauthorized collection of data from Facebook's network by third parties), Facebook is nevertheless aware that such scraping occurs, including of photos.

39. These risks can be especially dangerous for vulnerable populations, such as victims of domestic violence or stalking. Even those who have taken safety precautions by, *e.g.*, shielding information about their environs and patterns at work or home, may be "outed" by photo tagging without their knowledge. Given the lack of informed consent about Facebook's facial recognition program, vulnerable users cannot be assumed to somehow know or learn about the facial template and tagging features of Facebook. Another potential misuse involves discrimination or profiling based on race, religion, gender, or national origin.

40. The list of potential abuses of this powerful technology when paired with a database of personal information such as Facebook has amassed is long, and Facebook has been aware of these privacy concerns for years. For example, in December 2011, the FTC hosted a workshop to address the privacy and security issues associated with facial recognition technology. Following the workshop, the FTC issued a notice seeking public comments on issues raised during the discussion, including the privacy and security implications raised by the increasing use of facial recognition technology. In response to the FTC's public notice, the Electronic Privacy Information Center, a non-profit research center, submitted comments to the FTC that critiqued Facebook's use and collection of facial-feature data from its users.

41. The fact that Facebook has spent years of work and millions of dollars developing and implementing this technology, with full awareness of the above-described risks and privacy concerns, knowingly decided to implement the PTS program without meaningful user consent or even meaningful notice to their members before creating and analyzing their face templates on a massive scale, exhibits an extreme degree of recklessness towards the privacy of its members. The collection of biometric facial data by the PTS program, and the lack of transparency or consent associated with it, was clearly a calculated decision in which Facebook determined that the value of increased user engagement through the PTS program outweighed either the privacy rights of its members or the legal risks. Facebook must now live with the consequences of that decision under the BIPA and compensate its members (and affected non-members) for its intentional conduct under 740 ILCS 14/20(1).

42. Alternatively, Facebook's conduct was at the very least negligent, and liable under 740 ILCS 14/20(2).

VI. Plaintiff's Privacy Rights were Violated by Facebook's Photo Tag Suggest

43. Plaintiff Adam Pezen has been a resident of Chicago, Illinois since 2011. Plaintiff has been a member of Facebook continuously since 2005. Since he joined Facebook, Plaintiff has uploaded and posted many photographs to Facebook's network that include images of his face, and has tagged many of these photographs to identify himself in them. He has also been in many photographs (which included images of his face) that other Facebook members have uploaded and tagged him in.

44. Using these manually tagged images of Plaintiff, Facebook created a biometric facial template of Plaintiff's face that Facebook stores and uses without providing him access to it.

45. Plaintiff never provided informed consent, in writing or otherwise, to Facebook's creation, use or storage of his face template or any of his biometric information. Plaintiff has never even been provided with notice by Facebook that it was collecting or using his biometric face template information.

CLASS ALLEGATIONS

46. Plaintiff Adam Pezen is similarly situated to an overwhelming number of other Illinois residents that also had their biometric information collected by Facebook without notice or written consent in violation of the BIPA. Plaintiff therefore brings this class action pursuant to Fed. R. Civ. Pro. 23 on behalf of himself and a class of other similarly situated individuals (the "Class"), defined specifically as follows:

> **All persons who have had their biometric information collected, captured, received or otherwise obtained by Facebook while residing in Illinois.**

47. Excluded from the Class are the Defendants; the members of the immediate families of the Individual Defendants; the subsidiaries and affiliates of Defendants; any person

who is an officer, director, partner or controlling person of Facebook, including any of its subsidiaries or affiliates; any entity in which any Defendant has a controlling interest; and the legal representatives, heirs, successors and assigns of any such excluded person or entity.

48. The exact number of Class members is unknown to Plaintiff at this time, but it is clear that individual joinder is impracticable. Defendant has collected, captured, received, or otherwise obtained biometric identifiers or biometric information from at least thousands (and potentially even millions) of individuals who fall into the definition of the Class. Ultimately, the Class members will be easily identified through Defendant's records.

49. There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

(i) whether Facebook collected, captured received or otherwise obtained biometric identifiers or biometric information from Plaintiff and the Class;

(ii) whether Facebook properly informed Plaintiff and the Class in accordance with the BIPA of the biometric collection before collecting and using their biometric identifiers or biometric information;

(iii) whether Facebook obtained informed written consent from Plaintiffs and the Class to collect, use, and store their biometrics identifiers or biometric information;

(iv) whether Facebook had and made available to the public, a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometrics information in compliance with the BIPA;

(v) whether Facebook used Plaintiff's and the Class's biometric identifiers or biometric information to identify them; and

(vi) whether Facebook's violations of the BIPA were committed intentionally, recklessly, or negligently.

50. Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel with substantial experience in prosecuting complex class actions, including consumer actions and class actions relating to technology and social media (including against Facebook). Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Class, and Defendant has no defenses unique to Plaintiff.

51. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the class could sustain the cost of such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this complaint, and present a tremendous burden for the courts and taxpayers. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be achieved.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/15(b)
(On Behalf of Plaintiff and the Class)

52. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

53. The BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (l) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . 740 ILCS 14/15(b) (emphasis added).

54. Facebook is a Delaware corporation and thus qualifies as a "private entity" under the BIPA. *See* 740 ILCS 14/10.

55. Plaintiff and the Class are individuals who had their "biometric identifiers" collected by Facebook's facial recognition software (in the form of their facial geometries extracted from uploaded digital photographs), as explained in detail in Sections II-VI, above. *See* 740 ILCS 14/10.

56. Plaintiff's and the Class's biometric identifiers were used to identify them, and therefore constitute "biometric information" as defined by the BIPA. *See* 740 ILCS 14/10.

57. Facebook systematically collected, used, and stored their biometric identifiers or biometric information without first obtaining the specific written release required by 740 ILCS 14/15(b)(3).

58. In fact, as explained above, Facebook didn't properly inform Plaintiff or the class in writing that their biometric identifiers or biometric information were being collected and stored, nor did it inform them in writing of the specific purpose and length of term for which

their biometric identifiers or biometric information was being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

59. By collecting, storing, and using Plaintiffs and the Class's biometric identifiers and biometric information as described herein, Facebook violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in the BIPA, 740 ILCS 14/1, *et seq*.

60. On behalf of himself and the Class, Plaintiff seeks: (l) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Facebook to comply with the BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (2) statutory damages of $5,000 per violation for the intentional and reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000 per violation pursuant to 740 ILCS 14/20(1) if the Court finds that Facebook's violations were negligent; and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION
Violation of 740 ILCS 14/15(a)
(On Behalf of Plaintiff and the Class)

61. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

62. Section 15(a) of the BIPA requires that any "private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."

63. Facebook does not publicly provide a retention schedule or guidelines for permanently destroying its users' biometric identifiers and biometric information as specified by the BIPA.

64. By failing to develop and make publicly available a compliant policy and procedure for the destruction of its users' biometric information, Facebook has violated the rights of Plaintiff and the Class under Section 15(a) of the BIPA.

65. Accordingly, on behalf of himself and the Class, Plaintiff seeks: (i) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Facebook to establish and make publicly available a policy for the permanent destruction of biometric identifiers and biometric information that is compliant with 740 ILCS 14/15(a); (ii) statutory damages of $5,000 per violation for the intentional and reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000 per violation pursuant to 740 ILCS 14/20(1) if the Court finds that Facebook's violations were negligent; and (iii) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Adam Pezen, on behalf of himself and the Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing his counsel as Class Counsel;

B. Declaring that Facebook's actions, as set out above, violates the BIPA, 740 ILCS 14/1, *et seq.*;

C. Awarding statutory damages of $5,000 per violation for the intentional and reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000 per violation pursuant to 740 ILCS 14/20(1) if the Court finds that Facebook's violations were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, inter alia, an order requiring Facebook to collect, store, and use biometric identifiers or biometric information in compliance with the BIPA;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: April 21, 2015

LASKY & RIFKIND, LTD.,
Norman Rifkind
rifkind@laskyrifkind.com
Amelia S. Newton
newton@laskyrifkind.com

By: /s/ Norman Rifkind
351 W. Hubbard St., Suite 401
Chicago, IL 60654
(312) 634-0057

Local Counsel for Plaintiff

LABATON SUCHAROW LLP
Joel H. Bernstein
jbernstein@labaton.com

Corban S. Rhodes
crhodes@labaton.com
Ross M. Kamhi
rkamhi@labaton.com
140 Broadway
New York, NY 10005
(212) 907-0700

Attorneys for Plaintiff Adam Pezen